

ON ALGEBRAS ADMITTING A COMPLETE SET OF NEAR WEIGHTS, EVALUATION CODES AND GOPPA CODES

Cícero Carvalho¹ and Ercílio Silva²

Abstract. In 1998 Høholdt, van Lint and Pellikaan introduced the concept of a “weight function” defined on a \mathbb{F}_q -algebra and used it to construct linear codes, obtaining among them the algebraic-geometric (AG) codes supported on one point. Later, in 1999, it was proved by Matsumoto that all codes produced using a weight function are actually AG codes supported on one point. Recently, “near weight functions” (a generalization of weight functions), also defined on a \mathbb{F}_q -algebra, were introduced to study codes supported on two points. In this paper we show that an algebra admits a set of m near weight functions having a compatibility property, namely, the set is a “complete set”, if and only if it is the ring of regular functions of an affine geometrically irreducible algebraic curve defined over \mathbb{F}_q whose points at infinity have a total of m rational branches. Then the codes produced using the near weight functions are exactly the AG codes supported on m points. A formula for the minimum distance of these codes is presented with examples which show that in some situations it compares better than the usual Goppa bound.

Index terms. near weight functions, evaluation codes, algebraic geometric codes

1 Introduction

In 1981 V.D. Goppa showed how to use algebraic curves to produce error correcting codes (v. [6]), and his construction opened a new area of research in coding theory. After a decade of studies, researchers started to wonder if it was possible to find a simpler way to produce these (so called) algebraic-geometric, or Goppa, codes, one of the earliest attempt being made by Blahut ([1]). In 1998 Høholdt et al. (v. [5]) presented a simple construction for error correcting codes, using an \mathbb{F} -algebra \mathbf{R} and what they called a *weight function* on \mathbf{R} , their construction clearly producing algebraic-geometric codes supported on one point. The theory presented in [5] was recently generalized (v. [12] and [2]) by replacing weight functions by other

¹Universidade Federal de Uberlândia, Faculdade de Matemática, Av. J.N. de Ávila 2160, 38408-100 Uberlândia – MG, Brazil. email: cicero@ufu.br. Research partially supported by FAPEMIG - grant CEX APQ-4716-5.01/07

²Universidade Federal do ABC, CMCC, Rua Santa Adélia 166, 09210-170 Santo André – SP, Brazil. email: ercilio@ufabc.edu.br.

functions on \mathbf{R} , called *near weights*. In the present work we study specially algebras that admit m near weight functions with the property of being “a complete set” (see Definition 2.2). We will characterize them as being the ring of regular functions of an affine geometrically irreducible algebraic curve whose points at infinity have a total of m rational branches, from this we conclude that the codes obtained from such algebras using the complete set of near weight functions are exactly the algebraic-geometric codes supported on m points (thus generalizing results in [10] and [11]).

In what follows we will denote by \mathbb{N}_0 the set of nonnegative integers. Let \mathbb{F} be a field and \mathbf{R} be a commutative ring that contains \mathbb{F} , i.e. an \mathbb{F} -algebra. Given a function $\rho : \mathbf{R} \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ let $\mathcal{U}_\rho := \{f \in \mathbf{R} \mid \rho(f) \leq \rho(1)\}$ and $\mathcal{M}_\rho := \{f \in \mathbf{R} \mid \rho(f) > \rho(1)\}$.

Definitions 1.1 We call ρ a *near order* function on \mathbf{R} (or *n-order* for short) if for any $f, g \in \mathbf{R}$ we have:

- (N0) $\rho(f) = -\infty \Leftrightarrow f = 0$;
- (N1) $\rho(\lambda f) = \rho(f) \ \forall \lambda \in \mathbb{F}^*$;
- (N2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$;
- (N3) if $\rho(f) < \rho(g)$ then $\rho(fh) \leq \rho(gh)$; if moreover $h \in \mathcal{M}_\rho$ then $\rho(fh) < \rho(gh)$;
- (N4) if $\rho(f) = \rho(g)$ and $f, g \in \mathcal{M}_\rho$ then there exists $\lambda \in \mathbb{F}^*$ such that $\rho(f - \lambda g) < \rho(f)$.

An *n-order* function is called a *near weight* (or *n-weight* for short) if it also satisfies the following condition.

- (N5) $\rho(fg) \leq \rho(f) + \rho(g)$ and equality holds when $f, g \in \mathcal{M}_\rho$.

A trivial way to define an *n-order* ρ on \mathbf{R} is to set $\rho(0) := -\infty$ and $\rho(f) = 1$ for all $f \in \mathbf{R}$, $f \neq 0$, then we have $\mathcal{M}_\rho = \emptyset$ and $\mathcal{U}_\rho = \mathbf{R}$. We want to avoid such functions, so we say that an *n-order* ρ is *trivial* if $\mathcal{M}_\rho = \emptyset$ and from now on we work only with nontrivial *n-order* functions.

From (N3) it follows that \mathcal{M}_ρ does not have zero divisors, we also get the following results (cf. [2, Lemma 4]).

Lemma 1.2 *Let ρ be an *n-order* on \mathbf{R} , then:*

- i) the element λ in (N4) is uniquely determined;*
- ii) if $\rho(f) \neq \rho(g)$ then $\rho(f + g) = \max\{\rho(f), \rho(g)\}$.*

Notation. In the next sections we deal with subsets of \mathbb{N}_0^m , and will use the following conventions: we denote by $\mathbf{0}$ the m -tuple having all entries equal to zero;

when we write $\mathbf{a} \in \mathbb{N}_0^m$ it's to be understood that the entries of the m -tuple \mathbf{a} are $\mathbf{a} := (a_1, \dots, a_m)$ (similarly for $\mathbf{b}, \mathbf{c} \in \mathbb{N}_0^m$); we write sometimes $\mathbf{a}_i \in \mathbb{N}_0^m$, being then understood that $\mathbf{a}_i = (a_{i1}, \dots, a_{im})$. Also, for $i \in \{1, \dots, m\}$ we denote by \mathbf{e}_i the m -tuple that has all entries equal to zero, except the i -th entry, which is equal to 1. We add m -tuples and multiply them by nonnegative integers in the usual way.

2 Codes from near weights

In this section we show how to construct codes from algebras that admit a complete set of n -weights, and give a lower bound for their minimum distance. We begin by introducing the concept of normalized n -orders.

Definition 2.1 Let ρ be an n -order function, we define the *normalization* ρ' of ρ as being the function $\rho' : \mathbf{R} \rightarrow \mathbb{N}_0 \cup \{-\infty\}$ defined by $\rho'(0) = -\infty$, $\rho'(f) := 0$ if $f \in \mathcal{U}_\rho \setminus \{0\}$ and $\rho'(f) := \rho(f)$ if $f \in \mathcal{M}_\rho$.

From the proof of [2, Proposition 1] we know that ρ' is an n -order, $\mathcal{U}_{\rho'} = \mathcal{U}_\rho$ and $\mathcal{M}_{\rho'} = \mathcal{M}_\rho$. From now on we work only with normalized n -orders. If ρ is an n -weight then from (N5) we see that \mathcal{U}_ρ is a subalgebra of \mathbf{R} .

In this section we will show how to construct linear codes from \mathbb{F} -algebras and a set of n -weights which have a compatibility property which we define now. Let $\{\rho_1, \dots, \rho_m\}$ be a set of (nontrivial, normalized) n -weights.

Definition 2.2 We say that $\{\rho_1, \dots, \rho_m\}$ is a *complete set of n -weights for \mathbf{R}* if $\bigcap_{i=1}^m \mathcal{U}_{\rho_i} = \mathbb{F}$ and for all $k \in \{1, \dots, m\}$ we have that $\mathbb{N}_0 \setminus \rho_k(\bigcap_{1 \leq i \leq m; i \neq k} \mathcal{U}_{\rho_i})$ is a finite set.

Let \mathbf{R} be an \mathbb{F} -algebra that admits $\{\rho_1, \dots, \rho_m\}$ as a complete set of n -weights. Given $\mathbf{a} = (a_1, \dots, a_m) \in \mathbb{N}_0^m$ we define

$$\mathcal{L}(\mathbf{a}) := \{f \in \mathbf{R} : \rho_i(f) \leq a_i \ \forall i = 1, \dots, m\}.$$

From (N0), (N1) and (N2) we get that \mathcal{L} is an \mathbb{F} -vector subspace of \mathbf{R} .

Lemma 2.3 For any $k \in \{1, \dots, m\}$ we get $\mathcal{L}(\mathbf{a}) \subset \mathcal{L}(\mathbf{a} + \mathbf{e}_k)$; moreover $\dim(\mathcal{L}(\mathbf{a} + \mathbf{e}_k) / \mathcal{L}(\mathbf{a})) \leq 1$.

Proof: Assume that $f, g \in \mathcal{L}(\mathbf{a} + \mathbf{e}_k) \setminus \mathcal{L}(\mathbf{a})$, from (N4) we know that there exists $\lambda \in \mathbb{F}^*$ such that $\rho_k(f - \lambda g) \leq a_k$, and from (N1) and (N2) we get $\rho_i(f - \lambda g) \leq a_i$ for all $i \in \{1, \dots, m\} \setminus \{k\}$. Thus $f = \lambda g + h$ with $h \in \mathcal{L}(\mathbf{a})$ hence $\bar{f} = \lambda \bar{g}$ as elements of $\mathcal{L}(\mathbf{a} + \mathbf{e}_k)/\mathcal{L}(\mathbf{a})$. \square

Since $\mathcal{L}(\mathbf{0}) = \mathbb{F}$ we get as a corollary of the above lemma that $\mathcal{L}(\mathbf{a})$ is an \mathbb{F} -vector space of finite dimension for any $\mathbf{a} \in \mathbb{N}_0^m$.

For the remainder of this section, we will assume that \mathbb{F} is a finite field. Let $\varphi : \mathbf{R} \rightarrow \mathbb{F}^n$ be a surjective morphism of \mathbb{F} -algebras and let $\mathbf{a} \in \mathbb{N}_0^m$. We will denote by $C(\mathbf{a})$ the code $\varphi(\mathcal{L}(\mathbf{a}))$ and we want to determine a lower bound for the minimum distance of $C(\mathbf{a})^\perp$, in a way similar to that which has been done by Høholdt et alli in the case where $m = 1$ (cf. [5, Section 4]).

Definition 2.4 Let $k \in \{1, \dots, m\}$, and define $N_k(\mathbf{a})$ as a set of pairs of functions $\{(f_{k,1}, g_{k,1}), \dots, (f_{k,\ell_k}, g_{k,\ell_k})\}$ such that:

- a) $f_{k,i}, g_{k,i} \in \mathcal{L}(\mathbf{a} + \mathbf{e}_k)$ for all $i = 1, \dots, \ell_k$;
- b) $\rho_k(f_{k,i}) + \rho_k(g_{k,i}) = a_k + 1$;
- c) $\rho_k(f_{k,1}) < \dots < \rho_k(f_{k,\ell_k})$ (hence $\rho_k(g_{k,1}) > \dots > \rho_k(g_{k,\ell_k})$);
- d) given $s \in \{1, \dots, \ell_k - 1\}$ we have $f_{k,s}g_{k,r} \in \mathcal{L}(\mathbf{a})$ for all $r = s + 1, \dots, \ell_k$.

We will write $\nu_k(\mathbf{a}) := \#N_k(\mathbf{a})$.

Now, consider the matrices M and N , where the first ℓ_k rows of M are $\varphi(f_{k,1}), \dots, \varphi(f_{k,\ell_k})$, the first ℓ_k columns of N are $\varphi(g_{k,1}), \dots, \varphi(g_{k,\ell_k})$, and we complete the rows of M and the columns of N in a way such that $\text{rank}(M) = \text{rank}(N) = n$. Let $\mathbf{y} = (y_1, \dots, y_n) \in \mathbb{F}^n$ and let $D(\mathbf{y}) := (a_{ij})_{n \times n}$ where $a_{ij} = 0$ if $i \neq j$ and $a_{ii} = y_i$ for $i = 1, \dots, n$. Since $\text{rank}(M) = \text{rank}(N) = n$ we get $\text{rank}(MD(\mathbf{y})N) = \text{wt}(\mathbf{y})$; moreover if $r, s \in \{1, \dots, \ell_k\}$ then $(MD(\mathbf{y})N)_{r,s} = \mathbf{y} \cdot (\varphi(f_{k,r}) * \varphi(g_{k,s}))$, where \cdot is the usual inner product in \mathbb{F}^n and $*$ is the usual componentwise product that makes \mathbb{F}^n an \mathbb{F} -algebra.

Proposition 2.5 If $\mathbf{y} \in C(\mathbf{a})^\perp \setminus C(\mathbf{a} + \mathbf{e}_k)^\perp$ then $\text{rank}(MD(\mathbf{y})N) \geq \#N_k(\mathbf{a})$.

Proof: We have already noted that $(MD(\mathbf{y})N)_{r,s} = \mathbf{y} \cdot \varphi(f_{k,r}g_{k,s})$ for all $r, s \in \{1, \dots, \ell_k\}$. From definition 2.4 (d) we get that the $\ell_k \times \ell_k$ minor at the upper left corner of $MD(\mathbf{y})N$ is a lower triangular matrix. Since $f_{k,s}g_{k,s} \in \mathcal{L}(\mathbf{a} + \mathbf{e}_k) \setminus \mathcal{L}(\mathbf{a})$ from Lemma 2.3 we get $\dim \mathcal{L}(\mathbf{a} + \mathbf{e}_k) = \dim \mathcal{L}(\mathbf{a}) + 1$ hence $\mathbf{y} \cdot \varphi(f_{k,s}g_{k,s}) \neq 0$ for all $s = 1, \dots, \ell_k$. \square

Definition 2.6 Let $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^m$ be such that $a_i \leq b_i$ for all $i = 1, \dots, m$. We call a *path from \mathbf{a} to \mathbf{b}* a finite sequence of m -tuples $\mathcal{P} := (\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_r)$, where $\mathbf{a}_i \in \mathbb{N}_0^m$ for all $i \in \{0, \dots, r\}$, $\mathbf{a}_0 = \mathbf{a}$, $\mathbf{a}_r = \mathbf{b}$ and for any $i \in \{0, \dots, r-1\}$ we have $\mathbf{a}_{i+1} = \mathbf{a}_i + \mathbf{e}_{p(i)}$ for some $p(i) \in \{1, \dots, m\}$ which is called the *step place* of $\mathbf{a}_i \in \mathcal{P}$.

Lemma 2.7 Let $\mathbf{a} \in \mathbb{N}_0^m$, then there exists $\mathbf{b} \in \mathbb{N}_0^m$ such that $\dim C(\mathbf{b}) = n$ and $a_i \leq b_i$ for all $i \in \{1, \dots, m\}$.

Proof: Since φ is surjective there are $f_1, \dots, f_n \in \mathbf{R}$ such that $\{\varphi(f_1), \dots, \varphi(f_n)\}$ is a basis for \mathbb{F}^n , so it suffices to take $b_i := a_i + \max\{\rho_i(f_1), \dots, \rho_i(f_n)\}$, where $i \in \{1, \dots, m\}$ and set $\mathbf{b} := (b_1, \dots, b_m)$. \square

As a consequence of the above results we have the following bound for the minimum distance of $C(\mathbf{a})^\perp$.

Corollary 2.8 Let $\mathbf{a} \in \mathbb{N}_0^m$ and let $\mathbf{b} \in \mathbb{N}_0^m$ be such that $a_i \leq b_i$ for all $i \in \{1, \dots, m\}$ and $\dim C(\mathbf{b}) = n$. Given a path $\mathcal{P} = (\mathbf{a}_0, \dots, \mathbf{a}_r)$ from \mathbf{a} to \mathbf{b} the minimum distance of $C(\mathbf{a})^\perp$ is bounded from below by $\min\{\nu_{p(i)}(\mathbf{a}_i) \mid i = 0, \dots, r-1\}$.

At first glance a major drawback of the above result is that it depends on finding $\mathbf{b} \in \mathbb{N}_0^m$ such that $\dim \varphi(\mathcal{L}(\mathbf{b})) = n$, while we would like a bound that does not depend on the knowledge of φ . The following considerations show that we do not have to find such \mathbf{b} in order to calculate a bound.

Let $k \in \{1, \dots, m\}$, from (N5) we get that $\mathcal{S}_k := \rho_k(\cap_{1 \leq i \leq m; i \neq k} \mathcal{U}_{\rho_i})$ is a subsemigroup of \mathbb{N}_0 and since $\{\rho_1, \dots, \rho_m\}$ is a complete set for \mathbf{R} we get $\#(\mathbb{N}_0 \setminus \mathcal{S}_k) < \infty$ (i.e. \mathcal{S}_k is a numerical semigroup). Observe also that given $\mathbf{a} \in \mathbb{N}_0^m$ and $t_1, t_2 \in \mathcal{S}_k$ such that $t_1 + t_2 = a_k + 1$ then taking $f_1, f_2 \in \cap_{1 \leq i \leq m; i \neq k} \mathcal{U}_{\rho_i}$ such that $t_i = \rho_k(f_i)$, $i = 1, 2$, we get $(f_1, f_2) \in N_k(\mathbf{a})$ (of course also $(f_2, f_1) \in N_k(\mathbf{a})$, if $t_2 \neq t_1$).

Lemma 2.9 Let S be a numerical subsemigroup of \mathbb{N}_0 of genus g , let c be the conductor of S and let $u \in \mathbb{N}_0$. If $N := \{(a, b) : a, b \in S \setminus \{0\}; a + b = 2c + u\}$ then $\#N = 2(c - g) + u - 1$.

Proof: We have $2(c - 1 - g)$ pairs $(a, b) \in N$ such that either $1 \leq a \leq c - 1$ or $1 \leq b \leq c - 1$. And we have $u + 1$ pairs $(a, b) \in N$ with $c \leq a, b \leq c + u$. \square

Let $\mathbf{a} \in \mathbb{N}_0^m$ and let $(\mathbf{a}_i)_{i \in \mathbb{N}_0} \in \mathbb{N}_0^m$ be a sequence of m -tuples such that $\mathbf{a} = \mathbf{a}_0$, $\mathbf{a}_{i+1} = \mathbf{a}_i + \mathbf{e}_{p(i)}$ for some $p(i) \in \{1, \dots, m\}$ and $\lim_{i \rightarrow \infty} a_{ij} = \infty$, for all $j \in$

$\{1, \dots, m\}$ and all $i \in \mathbb{N}_0$. From (the proof of) Lemma 2.7 we know that there exists $r \in \mathbb{N}_0$ such that $\dim C(\mathbf{a}_r) = n$. For $k \in \{1, \dots, m\}$, let c_k be the conductor of \mathcal{S}_k , to calculate the bound indicated in Corollary 2.8 we should calculate $\nu_{p(i)}(\mathbf{a}_i)$ for all $i \in \{0, r-1\}$, but we observe that:

- a) if $\nu_k(\mathbf{a}) =: h > 2(c_k - g_k) - 1$ then set $u := h - 2(c_k - g_k) + 1$; we shall calculate $\nu_k(\mathbf{a}_i)$ at most for m -tuples \mathbf{a}_i such that $a_{i,k} \leq 2c_k + u - 1$ (in fact, if $a_{i,k} + 1 > 2c_k + u$ we will get $\nu_k(\mathbf{a}_i) > h$);
- b) if $\nu_k(\mathbf{a}) \leq 2(c_k - g_k) - 1$ then we shall calculate $\nu_k(\mathbf{a}_i)$ at most for m -tuples \mathbf{a}_i such that $a_{i,k} \leq 2c_k - 1$ (in fact, if $a_{i,k} + 1 > 2c_k$ then $\nu_k(\mathbf{a}_i) > 2(c_k - g_k) + 1$).

Thus we do not have to know r to calculate the bound.

The next result shows that geometric Goppa codes supported in m points are instances of the codes we described above.

Theorem 2.10 *Let \mathcal{X} be a nonsingular, geometrically irreducible, projective algebraic curve defined over \mathbb{F} , and let $G := \sum_{i=1}^m a_i Q_i$ and $D := P_1 + \dots + P_n$ be divisors on \mathcal{X} such that $\text{supp}(G) \cap \text{supp}(D) = \emptyset$ and P_i is a rational point, for all $i = 1, \dots, n$ (hence the Goppa code $C_{\mathcal{L}}(D, G)$ is the set of m -tuples $(h(P_1), \dots, h(P_n))$, where $h \in L(G)$). Then taking $\mathbf{R} := \cap_{Q \in \mathcal{X}; Q \neq Q_1, \dots, Q_m} \mathcal{O}_Q$, where \mathcal{O}_Q is the local ring at $Q \in \mathcal{X}$, and defining $\varphi(f) := (f(P_1), \dots, f(P_n))$ there exists a complete set of m near weights on \mathbf{R} such that $C_{\mathcal{L}}(D, G) = C(\mathbf{a})$, where $\mathbf{a} := (a_1, \dots, a_m)$.*

Proof: Observe that \mathbf{R} is the \mathbb{F} -subalgebra of $\mathbb{F}(\mathcal{X})$ consisting of the functions regular on $\mathcal{X}' := \mathcal{X} \setminus \{Q_1, \dots, Q_m\}$. Denoting by v_k the discrete valuation of $\mathbb{F}(\mathcal{X})$ associated to Q_k ($k \in \{1, \dots, m\}$), one easily checks that the function $\rho_k : \mathbf{R} \rightarrow \mathbb{N}_0 \cup \{\infty\}$ defined by $\rho_k(0) = -\infty$, $\rho_k(f) = 0$ if $v_k(f) \geq 0$ and $\rho_k(f) = -v_k(f)$ if $v_k(f) < 0$, for all $f \in \mathbf{R} \setminus \{0\}$ is an n -weight for all $k \in \{1, \dots, m\}$. We have $\mathcal{U}_{\rho_k} = \mathbf{R} \cap \mathcal{O}_{Q_k}$ and $\mathcal{M}_k = \mathbf{R} \setminus \mathcal{O}_{Q_k}$ for all $k \in \{1, \dots, m\}$. Moreover, since $\cap_{Q \in \mathcal{X}} \mathcal{O}_Q = \mathbb{F}$ (because \mathcal{X} is geometrically irreducible) and $\mathcal{S}_k := \rho_k(\cap_{1 \leq i \leq m; i \neq k} \mathcal{U}_{\rho_i}) = \rho_k(\cap_{Q \in \mathcal{X}, Q \neq Q_k} \mathcal{O}_Q)$ is the Weierstrass semigroup at Q_k for all $k \in \{1, \dots, m\}$ (hence it has finite genus) we get that $\{\rho_1, \dots, \rho_m\}$ is a complete set of n -weights for \mathbf{R} .

Denoting by M_{P_i} the maximal ideal of \mathcal{O}_{P_i} we get that $\mathbf{R}/(M_{P_i} \cap \mathbf{R}) \cong \mathcal{O}_{P_i}/M_{P_i}$ for all $i \in \{1, \dots, n\}$ (see e.g. [13, Prop. III.2.9]), hence $\mathbb{F}^n \cong \mathbf{R}/(M_{P_1} \cap \mathbf{R}) \times \dots \times \mathbf{R}/(M_{P_n} \cap \mathbf{R})$ and from the Chinese Remainder Theorem φ is an epimorphism. We also have $\mathcal{L}(\mathbf{a}) = \{f \in \mathbf{R} \mid -v_k(f) \leq a_k, k = 1, \dots, m\} = \{f \in \mathbb{F}(\mathcal{X})^* \mid \text{div}(f) + \sum_{i=1}^m a_i Q_i \geq 0\} \cup \{0\} = L(G)$ hence $C(\mathbf{a}) = C_{\mathcal{L}}(D, G)$. \square

Now we present examples which show that when applied to a geometric Goppa code, the bound for the minimum distance found above may be better than the usual Goppa bound.

Examples 2.11 Let \mathcal{X} be the hermitian curve given by $Y^3Z + YZ^3 - X^4 = 0$ and defined over the field \mathbb{F}_{3^2} . Take Q_1, Q_2 and Q_3 to be three distinct rational points, say the points in the intersection of \mathcal{X} , the open set $Z \neq 0$ and the line $X = 0$, let $\mathbf{a} := (a_1, a_2, a_3) \in \mathbb{N}_0^3$ and denote by $\mathcal{C}_{\mathcal{L}}(D, G_{\mathbf{a}})$ the geometric Goppa code associated to the divisors $G_{\mathbf{a}} := a_1Q_1 + a_2Q_2 + a_3Q_3$ and $D = P_1 + \dots + P_n$, where P_1, \dots, P_n are distinct rational points, different from Q_1, Q_2 and Q_3 . The genus of \mathcal{X} is 3 and the so-called Goppa bound for the code $\mathcal{C}_{\mathcal{L}}(D, G_{\mathbf{a}})^{\perp}$ is $d_{\mathbf{a}} := \deg G_{\mathbf{a}} - (2g - 2) = \sum_{i=1}^3 a_i - 4$. Note that \mathcal{S}_i is the semigroup generated by 3 and 4, so the conductor is 6, for all $k = 1, 2, 3$. To find a bound as described in Corollary 2.8 it is useful to know the set $\{(\rho_1(f), \rho_2(f), \rho_3(f)) \in \mathbb{N}_0^3 \mid f \in \mathbf{R}\}$, which in this case is exactly the Weierstrass semigroup \mathcal{W} associated to $\{Q_1, Q_2, Q_3\}$, i.e. the set $\mathcal{S} = \{(n_1, n_2, n_3) \in \mathbb{N}_0^3 \mid \text{div}_{\infty}(f) = n_1Q_1 + n_2Q_2 + n_3Q_3\}$, where $\text{div}_{\infty}(f)$ denotes the pole divisor of f . Such semigroups have been much studied in the last decade (see e.g. [9], [8], [7], [3]), and in [7] we find an explicit description of a generating set for this semigroup, so that we may decide if an element of \mathbb{N}_0^3 is or is not in \mathcal{S} . Thus, given $\mathbf{a} \in \mathbb{N}_0^3$ we proceed as follows. For $k = 1, 2, 3$ we calculate $\nu_k(\mathbf{a})$, if $\nu_k(\mathbf{a}) > 2(6 - 3) - 1 = 5$ then set $A_k := 2 \cdot 6 + (\nu_k(\mathbf{a}) - 5) - 1$, if $\nu_k(\mathbf{a}) \leq 5$ then we set $A_k := 2 \cdot 6 - 1 = 11$. Let $r := \sum_{i=1}^3 (A_i - a_i)$ and consider the path \mathcal{P} from \mathbf{a} to (A_1, A_2, A_3) given by $(\mathbf{a}_0, \dots, \mathbf{a}_r)$ where $\mathbf{a}_0 = \mathbf{a}$, $\mathbf{a}_r = (A_1, A_2, A_3)$, $\mathbf{a}_i = \mathbf{a} + i\mathbf{e}_1$, for $i \in \{1, \dots, A_1 - a_1\}$, $\mathbf{a}_{A_1 - a_1 + j} = \mathbf{a} + (A_1 - a_1)\mathbf{e}_1 + j\mathbf{e}_2$, for $j \in \{1, \dots, A_2 - a_2\}$, and $\mathbf{a}_{A_1 - a_1 + A_2 - a_2 + k} = \mathbf{a} + (A_1 - a_1)\mathbf{e}_1 + (A_2 - a_2)\mathbf{e}_2 + k\mathbf{e}_3$, for $k \in \{1, \dots, A_3 - a_3\}$. From the considerations that precede these examples we get that $\delta_{\mathbf{a}} := \min\{\nu_{p(i)}(\mathbf{a}_i) \mid i = 0, \dots, r - 1\}$ is a bound for the minimum distance of $\mathcal{C}_{\mathcal{L}}(D, G_{\mathbf{a}})^{\perp}$.

Let $\boldsymbol{\rho}(N_k(\mathbf{a})) := \{((\rho_1(f_{k,i}), \rho_2(f_{k,i}), \rho_3(f_{k,i})), (\rho_1(g_{k,i}), \rho_2(g_{k,i}), \rho_3(g_{k,i}))) \mid i = 1, \dots, \ell_k\}$, taking $\mathbf{a} = (2, 1, 1)$ we have $\nu_1(\mathbf{a}) = 2$ (with $\boldsymbol{\rho}(N_1(\mathbf{a})) = \{((0, 0, 0), (3, 0, 0)), ((3, 0, 0), (0, 0, 0))\}$), $\nu_2(\mathbf{a}) = 2$ (with $\boldsymbol{\rho}(N_2(\mathbf{a})) = \{((0, 0, 0), (0, 3, 0)), ((0, 3, 0), (0, 0, 0))\}$), and $\nu_3(\mathbf{a}) = 3$ (with $\boldsymbol{\rho}(N_3(\mathbf{a})) = \{((0, 0, 0), (0, 2, 2)), ((1, 1, 1), (1, 1, 1)), ((0, 2, 2), (0, 0, 0))\}$).

Thus $(A_1, A_2, A_3) = (11, 11, 11)$ and inspecting \mathcal{W} we get that $\delta_{\mathbf{a}} = 2$, while $d_{\mathbf{a}} = 0$. In the table below we present results for this and other values of \mathbf{a} .

\mathbf{a}	$(\nu_1(\mathbf{a}), \nu_2(\mathbf{a}), \nu_3(\mathbf{a}))$	(A_1, A_2, A_3)	$\delta_{\mathbf{a}}$	$d_{\mathbf{a}}$
(2, 1, 1)	(2,2,2)	(11,11,11)	2	0
(1, 2, 1)	(2,2,2)	(11,11,11)	2	0
(1, 1, 2)	(2,2,2)	(11,11,11)	2	0
(2, 2, 1)	(2,2,3)	(11,11,11)	2	1
(2, 1, 2)	(2,3,2)	(11,11,11)	2	1
(1, 2, 2)	(3,2,2)	(11,11,11)	2	1
(2, 2, 2)	(3,3,3)	(11,11,11)	2	2
(3, 2, 2)	(4,4,4)	(11,11,11)	3	3
(2, 3, 2)	(4,4,4)	(11,11,11)	3	3
(2, 2, 3)	(4,4,4)	(11,11,11)	4	3

Table 1: Bounds for $\delta_{\mathbf{a}}$ and $d_{\mathbf{a}}$; code $C(\mathbf{a})^\perp$; curve $Y^3Z + YZ^3 - X^4 = 0$, defined over \mathbb{F}_9 .

We also present a similar table, containing examples of codes from the hermitian curve given by $Y^4Z + YZ^4 - X^5 = 0$ and defined over the field \mathbb{F}_{16} . Again, we take Q_1, Q_2 and Q_3 to be three distinct rational points of the curve, now \mathcal{S}_i is the semigroup generated by 4 and 5, so the conductor is 12, for $i = 1, 2, 3$; the genus of the curve is 6.

\mathbf{a}	$(\nu_1(\mathbf{a}), \nu_2(\mathbf{a}), \nu_3(\mathbf{a}))$	(A_1, A_2, A_3)	$\delta_{\mathbf{a}}$	$d_{\mathbf{a}}$
(1, 2, 3)	(2,2,2)	(23,23,23)	2	-4
(3, 1, 3)	(2,2,2)	(23,23,23)	2	-3
(3, 2, 3)	(2,2,2)	(23,23,23)	2	-2
(3, 3, 3)	(2,2,2)	(23,23,23)	2	-1
(4, 3, 2)	(2,2,2)	(23,23,23)	2	-1
(4, 3, 3)	(2,2,2)	(23,23,23)	2	0
(4, 4, 3)	(2,2,3)	(23,23,23)	2	1

Table 2: Bounds for $\delta_{\mathbf{a}}$ and $d_{\mathbf{a}}$; code $C(\mathbf{a})^\perp$; curve $Y^4Z + YZ^4 - X^5 = 0$; defined over \mathbb{F}_{16} .

3 Algebras with near weights and algebraic curves

In this section we present a characterization for algebras which admit a complete set of n-weights.

Lemma 3.1 *Let \mathbf{R} be an \mathbb{F} -algebra and ρ an n -weight. Let $f, g \in \mathbf{R}$ be such that $\rho(f) > 0$, $\rho(g) = 0$, $g \notin \mathbb{F}$ and $\rho(fg) < \rho(f)$. Then for any $\lambda \in \mathbb{F}^*$ we have $\rho(f(g + \lambda)) = \rho(f)$ and $\rho(g + \lambda) = 0$.*

Proof: Let $\lambda \in \mathbb{F}^*$, then $\rho(f(g + \lambda)) = \rho(fg + \lambda f) \leq \max\{\rho(fg), \rho(f)\}$. Since $\rho(fg) < \rho(f)$ we get $\rho(f(g + \lambda)) = \rho(f)$. We also have $g + \lambda \in \mathcal{U}_\rho$ since \mathcal{U}_ρ is an \mathbb{F} -subalgebra of \mathbf{R} . \square

Let \mathbf{R} be an \mathbb{F} -algebra which admits a (not necessarily complete) set of n -weights $\{\rho_1, \dots, \rho_m\}$. Let $\boldsymbol{\rho} : \mathbf{R} \setminus \{0\} \rightarrow \mathbb{N}_0^m$ be the map defined by $\boldsymbol{\rho}(f) := (\rho_1(f), \dots, \rho_m(f))$ and let $\mathcal{S}_{\rho_1, \dots, \rho_m} = \mathcal{S} := \boldsymbol{\rho}(\mathbf{R} \setminus \{0\})$.

We will always assume that if the field \mathbb{F} is finite then $\#(\mathbb{F}) \geq m$.

Definition 3.2 Let $\mathbf{a}_i \in \mathbb{N}_0^m$, with $i = 1, \dots, r$. We define the *least upper bound* of $\mathbf{a}_1, \dots, \mathbf{a}_r$ as being the m -tuple $\text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_r) := (b_1, \dots, b_m)$ where $b_j = \max\{a_{j1}, \dots, a_{jr}\}$ for all $j = 1, \dots, m$.

Proposition 3.3 *Let $\mathbf{a}_1, \dots, \mathbf{a}_r \in \mathcal{S}$, then $\text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_r) \in \mathcal{S}$. Furthermore, if $f_1, \dots, f_r \in \mathbf{R}$ are such that $\boldsymbol{\rho}(f_i) = \mathbf{a}_i$ for all $i \in \{1, \dots, r\}$ then there exists $f \in \mathbf{R}$, $f = \sum_{i=1}^r \lambda_i f_i$, where $\lambda_1, \dots, \lambda_r \in \mathbb{F}$ such that $\boldsymbol{\rho}(f) = \text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_r)$.*

Proof: Since $\text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_j) = \text{lub}(\text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_{j-1}), \mathbf{a}_j)$ for all $j = 2, \dots, r$ it suffices to prove the case where $r = 2$. Let $f, g \in \mathbf{R}$ be such that $\boldsymbol{\rho}(f) = \mathbf{a}_1$ and $\boldsymbol{\rho}(g) = \mathbf{a}_2$. If $\mathbf{a}_1 = \mathbf{a}_2$ then the result is trivial, so we will assume that $\mathbf{a}_1 \neq \mathbf{a}_2$, a fortiori $f \neq \lambda g$ for all $\lambda \in \mathbb{F}^*$. If $\#(\{j \mid a_{1j} = a_{2j}\}) = m - 1$ then $\text{lub}(\mathbf{a}_1, \mathbf{a}_2) \in \{\mathbf{a}_1, \mathbf{a}_2\}$, so we assume that $\#(\{j \mid a_{1j} = a_{2j}\}) \leq m - 2$. Let $i \in \{1, \dots, m\}$, if $\rho_i(f) \neq \rho_i(g)$ then $\rho_i(f + \lambda g) = \max\{\rho_i(f), \rho_i(g)\}$ for all $\lambda \in \mathbb{F}^*$; if $\rho_i(f) = \rho_i(g) = 0$ then for all $\lambda \in \mathbb{F}^*$ we get $\rho_i(f + \lambda g) = 0$; if $\rho_i(f) = \rho_i(g) \neq 0$ then there exists a unique $\lambda_i \in \mathbb{F}^*$ such that $\rho_i(f - \lambda_i g) < \rho_i(f)$, hence for all $\lambda \in \mathbb{F}^*$, $\lambda \neq -\lambda_i$ we get $\rho_i(f + \lambda g) = \rho_i(f)$. Since $\#(\mathbb{F}) - 1 > m - 2$ there exists $\lambda \in \mathbb{F}^*$ such that $\rho_i(f + \lambda g) = \max\{\rho_i(f), \rho_i(g)\}$ for all $i \in \{1, \dots, m\}$. \square

Lemma 3.4 *Let \mathbf{a} and \mathbf{b} be distinct elements of \mathcal{S} and suppose that $a_j = b_j$ for some $j \in \{1, \dots, m\}$. Then there exists $\mathbf{c} \in \mathcal{S}$ such that:*

- i) $c_i = \max\{a_i, b_i\}$ for $i \neq j$ and $a_i \neq b_i$;
- ii) $c_i \leq a_i$ for all $i \neq j$ and $a_i = b_i$;
- iii) $c_j = a_j = 0$ or $c_j < a_j$.

Proof: Let $f, g \in \mathbf{R}$ such that $\rho(f) = \mathbf{a}$ and $\rho(g) = \mathbf{b}$. If $a_j = b_j = 0$ then it suffices to take $\mathbf{c} = \rho(f + g)$. If $a_j = b_j > 0$ then $f, g \in \mathcal{M}_{\rho_j}$ and there exists $\lambda \in \mathbb{F}^*$ such that $\rho_j(f - \lambda g) < a_j$, so we take $\mathbf{c} = \rho(f - \lambda g)$. \square

Let \preceq be the (partial) ordering in \mathbb{N}_0^m given by the relation $\mathbf{a} \preceq \mathbf{b}$ if $a_i \leq b_i$ for all $i \in \{1, \dots, m\}$.

Proposition 3.5 *Let $\mathbf{a} \in \mathcal{S}$, then the following assertions are equivalent:*

- i) \mathbf{a} is a minimal element of the set $\{\mathbf{c} \in \mathcal{S} \mid c_k = a_k\}$ for some $k \in \{1, \dots, m\}$ such that $a_k > 0$;*
- ii) \mathbf{a} is a minimal element of the set $\{\mathbf{c} \in \mathcal{S} \mid c_i = a_i\}$ for all $i \in \{1, \dots, m\}$ such that $a_i > 0$.*

Proof: Assume that \mathbf{a} is a minimal of the set $\{\mathbf{c} \in \mathcal{S} \mid c_k = a_k\}$ for some $k \in \{1, \dots, m\}$ and suppose that \mathbf{a} is not a minimal of the set $\{\mathbf{c} \in \mathcal{S} \mid c_j = a_j\}$ for some $j \in \{1, \dots, m\}$. Then there exists $\mathbf{b} \in \mathcal{S}$ such that $\mathbf{b} \preceq \mathbf{a}$, $\mathbf{b} \neq \mathbf{a}$ and $b_j = a_j$, furthermore, from the hypothesis we must have $b_k < a_k$. From Lemma 3.4 there exists $\mathbf{c} \in \mathcal{S}$ such that $c_i \leq \max\{a_i, b_i\}$ for all $i \in \{1, \dots, m\}$, $c_k = a_k$ and $c_j < a_j$, so \mathbf{a} is not a minimal of the set $\{\mathbf{c} \in \mathcal{S} \mid c_k = a_k\}$, a contradiction. \square

Definition 3.6 If $\mathbf{a} \in \mathcal{S}$ is a minimal element of the set $\{\mathbf{c} \in \mathcal{S} \mid c_k = a_k\}$ for some $k \in \{1, \dots, m\}$ we say that \mathbf{a} is a *minimal* of \mathcal{S} (cf. [7, Section 2]). We will denote by Γ the set of all minimals.

Observe that $\mathbf{0}$ and the points of \mathcal{S} which have all entries but one equal to zero are minimals.

Theorem 3.7 *The set \mathcal{S} is a subsemigroup of \mathbb{N}_0^m .*

Proof: Let $\mathbf{a}, \mathbf{b} \in \mathcal{S}$ and let $f, g \in \mathbf{R}$ be such that $\rho(f) = \mathbf{a}$ and $\rho(g) = \mathbf{b}$. Set $\mathbf{c} := \rho(fg)$, for $i \in \{1, \dots, m\}$ we have $c_i \leq a_i + b_i$ and equality holds whenever $a_i > 0$ and $b_i > 0$, hence $\mathbf{a} + \mathbf{b} = \text{lub}(\mathbf{a}, \mathbf{b}, \mathbf{c})$. \square

We assume from now on that $\{\rho_1, \dots, \rho_m\}$ is a complete set of n-weights for \mathbf{R} ; the next result shows that Γ generates the semigroup \mathcal{S} under the operation lub .

Lemma 3.8 *Let $\mathbf{a} \in \mathcal{S}$ and let r be the number of nonzero entries of \mathbf{a} , then there exist $\mathbf{a}_1, \dots, \mathbf{a}_r \in \Gamma$ such that $\mathbf{a} = \text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_r)$.*

Proof: Let $\mathbf{a} \in \mathcal{S} \setminus \Gamma$ and let $\Lambda \subset \{1, \dots, m\}$ be the set of indexes i for which $\mathbf{a}_i > 0$; from Proposition 3.5 \mathbf{a} is not a minimal in any set $\{\mathbf{b} \in \mathcal{S} \mid b_i = a_i\}$ with $i \in \Lambda$, then for all $i \in \Lambda$ there exists $\mathbf{b}_i \in \Gamma$ such that $\mathbf{b}_i \preccurlyeq \mathbf{a}$ and $b_{ii} = a_i$, so we have $\mathbf{a} = \text{lub}(\mathbf{b}_i; i \in \Lambda)$. \square

Given $j \in \{1, \dots, m\}$ let $H_j := \{a \in \mathbb{N}_0 \mid \exists f \in \cap_{i=1; i \neq j}^m \mathcal{U}_{\rho_i} \text{ such that } \rho_j(f) = a\}$ (i.e. $a \in H_j$ if and only if there exists $\mathbf{a} \in \mathcal{S}$ having all entries equal to zero, except the j -th entry, which is equal to a). Then H_j is a semigroup which has finite genus (since $\{\rho_1, \dots, \rho_m\}$ is a complete set of n -weights).

Lemma 3.9 *Let $\mathbf{a} \in \Gamma$ and let $\Lambda = \{j \mid a_j > 0\} \subset \{1, \dots, m\}$. If $\#\Lambda \geq 2$ then $a_j \notin H_j$ for all $j \in \Lambda$.*

Proof: Let $j \in \Lambda$ and assume by means of absurd that $a_j \in H_j$; let $\mathbf{b} \in \mathbb{N}_0^m$ be the m -tuple having all entries equal to zero except the j -th, which is equal to a_j . Then $\mathbf{b} \in \mathcal{S}$, $\mathbf{b} \preccurlyeq \mathbf{a}$ and $\mathbf{b} \neq \mathbf{a}$, hence $\mathbf{a} \notin \Gamma$. \square

Let $\tilde{\Gamma} := \{\mathbf{a} \in \Gamma \mid \mathbf{a} \text{ has at least two nonzero entries}\}$, an easy but important consequence of the above lemma is the following.

Corollary 3.10 *The set $\tilde{\Gamma}$ is finite.*

Proof: Let G_j be the set of gaps of H_j , then $\#(G_j) < \infty$ for all $j \in \{1, \dots, m\}$ and from the lemma above $\tilde{\Gamma} \subset G_1 \times \dots \times G_m$. \square

For each $\mathbf{a} \in \Gamma$ let $f_{\mathbf{a}} \in \mathbf{R}$ be such that $\boldsymbol{\rho}(f_{\mathbf{a}}) = \mathbf{a}$, and let $\mathcal{B} := \{f_{\mathbf{a}} \in \mathbf{R}; \mid \mathbf{a} \in \Gamma\}$.

Proposition 3.11 *The set \mathcal{B} spans \mathbf{R} as an \mathbb{F} -vector space.*

Proof: We want to show that any $f \in \mathbf{R} \setminus \{0\}$ is a finite linear combination over \mathbb{F} of elements of \mathcal{B} , and we do this by induction on the number of nonzero entries of $\mathbf{a} := \boldsymbol{\rho}(f)$. If this number is zero then $f \in \mathbb{F}^*$ and is a multiple of $f_0 \in \mathbb{F}^*$. Assume that \mathbf{a} has r nonzero entries, with $r \geq 1$, and for simplicity, let's assume that these entries are a_1, \dots, a_r . From Lemma 3.8 there are $\mathbf{a}_1, \dots, \mathbf{a}_r \in \Gamma$ such that $\mathbf{a} = \text{lub}(\mathbf{a}_1, \dots, \mathbf{a}_r)$ and from Proposition 3.3 there are $\lambda_1, \dots, \lambda_r \in \mathbb{F}$ such that $g := \sum_{i=1}^r \lambda_i f_{\mathbf{a}_i}$ satisfies $\boldsymbol{\rho}(g) = \boldsymbol{\rho}(f)$. Since $\rho_1(f) = \rho_1(g) = a_1 > 0$ there is $\lambda \in \mathbb{F}^*$ such that $\rho_1(f - \lambda g) < a_1$, moreover $\rho_j(f - \lambda g) \leq a_j$ for all $j \in \{2, \dots, m\}$. If $f = \lambda g$ we are done, otherwise we repeat the process, starting with $f - \lambda g$ this time, until we get either that f is a linear combination of finite elements of \mathcal{B} or

that the m -tuple obtained by applying the function ρ to f minus a finite linear combination of elements of \mathcal{B} has less than r nonzero elements (because the first entry is certainly zero); either way we're done. \square

Proposition 3.12 \mathbf{R} is a finitely generated algebra over \mathbb{F} .

Proof: Let $i \in \{1, \dots, m\}$, we know that the semigroup $H_i \subset \mathbb{N}_0$ has finite genus, hence it is finitely generated, so let $H_i = \langle a_{i1}, \dots, a_{ir_i} \rangle$. For each a_{ij} with $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, r_i\}$ there is $\mathbf{a}_{ij} \in \Gamma$ having all entries equal to zero, except the i -th entry which is equal to a_{ij} . Thus if $\mathbf{a} \in \Gamma \setminus \tilde{\Gamma}$, i.e. if \mathbf{a} has only one positive entry, which is in the i -th position for some $i \in \{1, \dots, m\}$, then for certain $\alpha_1, \dots, \alpha_{r_i} \in \mathbb{N}_0$ we have $\rho(f_{\mathbf{a}_{i1}}^{\alpha_1} \dots f_{\mathbf{a}_{ir_i}}^{\alpha_{r_i}}) = \mathbf{a}$ (recall that $f_{\mathbf{a}_{ij}} \in \mathcal{B}$ and are such that $\rho(f_{\mathbf{a}_{ij}}) = \mathbf{a}_{ij}$ for all $j \in \{1, \dots, r_i\}$) and we can take $f_{\mathbf{a}} := f_{\mathbf{a}_{i1}}^{\alpha_1} \dots f_{\mathbf{a}_{ir_i}}^{\alpha_{r_i}}$. Since $\tilde{\Gamma}$ is a finite set, the result follows from the above proposition. \square

Theorem 3.13 Let $f \in \mathbf{R}$, $f \neq 0$, then $\dim_{\mathbb{F}} \mathbf{R}/(f) < \infty$.

Proof: We may assume that $f \in \mathbf{R} \setminus \mathbb{F}$. We also assume $m \geq 2$ (for $m = 1$ the proof is in [10]). From Proposition 3.11 we have that the set $\overline{\mathcal{B}} := \{\overline{f_{\mathbf{a}}} \in \mathbf{R}/(f) \mid \mathbf{a} \in \Gamma\}$ spans $\mathbf{R}/(f)$ as a vector space over \mathbb{F} , and since $\tilde{\Gamma}$ is finite, it suffices to show that for all $\mathbf{a} \in \Gamma \setminus \tilde{\Gamma}$, except maybe for a finite number, we may take $f_{\mathbf{a}} \in (f)$. Thus, we will show that for any $i \in \{1, \dots, m\}$ there exists $n_i \in \mathbb{N}_0$ such that for all $n \geq n_i$ with $n \in H_i$ we may find $s \in (f)$ such that $\rho_i(s) = n$ and $\rho_j(s) = 0$ for all $j \in \{1, \dots, m\}$, $j \neq i$. For simplicity, let's take $i = 1$; we will consider two cases. In the first case, we assume that $\rho_j(f) = 0$ for all $j = 2, \dots, m$, hence $\rho_1(f) > 0$ (since $f \notin \mathbb{F}$). Let ℓ_1 be the largest gap of H_1 and set $d_1 := \rho_1(f)$, if a_{11}, \dots, a_{1r_1} are generators for H_1 , then using the notation of the preceding proof, for any $n > \ell_1 + d_1$ we may find $\alpha_1, \dots, \alpha_{r_1} \in \mathbb{N}_0$ such that $\rho_1(f_{\mathbf{a}_{11}}^{\alpha_1} \dots f_{\mathbf{a}_{1r_1}}^{\alpha_{r_1}} f) = n$ and $\rho_j(f_{\mathbf{a}_{11}}^{\alpha_1} \dots f_{\mathbf{a}_{1r_1}}^{\alpha_{r_1}} f) = 0$ for all $j = 2, \dots, m$. In the second case we assume that there exists $j \in \{2, \dots, m\}$ such that $\rho_j(f) > 0$. Let $g \in \mathbf{R}$ be such that $\rho_1(g) > 0$ and $\rho_i(g) = 0$ for all $i \in \{2, \dots, m\}$ (such g exists because the genus of H_1 is finite, moreover $g \notin \mathbb{F}$), then $\rho_j(fg) \leq \rho_j(f)$ and there exists $\lambda \in \mathbb{F}$ such that $\rho_j(fg - \lambda f) = \rho_j(f(g - \lambda)) < \rho_j(f)$. We have $g - \lambda \in \mathcal{M}_{\rho_1}$ but for all $i \in \{2, \dots, m\}$, since $g \in \mathcal{U}_{\rho_i}$ we have $g - \lambda \in \mathcal{U}_{\rho_i}$ and $\rho_i(f(g - \lambda)) \leq \rho_i(f)$. By repeating this process we may find $h \in \mathcal{M}_{\rho_1}$ such that $\rho_i(hf) \leq \rho_i(f)$ for all

$i \in \{2, \dots, m\}$ and $\rho_j(hf) = 0$; repeating even further we find $t \in \mathcal{M}_{\rho_1}$ such that $\rho_i(tf) = 0$ for all $i \in \{2, \dots, m\}$ (observe that $\rho_1(tf) > 0$ since if $\rho_1(tf) = 0$ then $tf \in \cap_{i=1}^m \mathcal{U}_{\rho_i} = \mathbb{F}$, and a fortiori $f \in \mathbb{F}$, a contradiction). Let ℓ_1 be the largest gap in H_1 and set $d_1 := \rho_1(tf)$; given $n > \ell_1 + d_1$ let $u \in \mathcal{M}_{\rho_1}$ be such that $\rho_1(u) = n - d_1$ and $\rho_i(u) = 0$ for all $i \in \{2, \dots, m\}$, then $\rho_1(utf) = n$ and $\rho_i(utf) = 0$ for all $i \in \{2, \dots, m\}$. This completes the proof. \square

We have already observed that \mathbf{R} is a domain, and we will denote by \mathbf{K} its field of fractions.

Lemma 3.14 *\mathbf{K} is an algebraic function field of one variable over \mathbb{F} .*

Proof: Let $f \in \mathbf{R}$, $f \neq 0$, from Theorem 3.13 we know that $\mathbf{R}/(f)$ is an \mathbb{F} -vector space of finite dimension, furthermore, all ideals of $\mathbf{R}/(f)$ are \mathbb{F} -subspaces hence $\mathbf{R}/(f)$ is an artinian ring, so $\dim_{\mathbf{K}^{\text{rull}}} \mathbf{R}/(f) = 0$. Taking $f \in \mathbf{R} \setminus \mathbb{F}$, from [4, Corollary 13.11] we have $\dim_{\mathbf{K}^{\text{rull}}} \mathbf{R} = \dim_{\mathbf{K}^{\text{rull}}} \mathbf{R}/(f) + 1$; on the other hand from [4, Theorem A, page 223] we get $\text{tr deg}_{\mathbb{F}} \mathbf{K} = \dim_{\mathbf{K}^{\text{rull}}} \mathbf{R} = 1$. \square

Corollary 3.15 *The algebra \mathbf{R} is the affine coordinate ring of an (irreducible) algebraic curve.*

Proof: It is an immediate consequence of Proposition 3.12 and the above lemma. \square

Let $i \in \{1, \dots, m\}$, from the proof of Theorem 3.13 we get that if $f \in \mathbf{R} \setminus \{0\}$ then there exists $g \in \mathcal{M}_{\rho_i}$ such that $gf \in \mathcal{M}_{\rho_i}$, hence if $a, b \in \mathbf{R} \setminus \{0\}$ and $g_1a, g_2b \in \mathcal{M}_{\rho_i}$ with $g_1, g_2 \in \mathcal{M}_{\rho_i}$ then $(g_1g_2)a, (g_1g_2)b \in \mathcal{M}_{\rho_i}$.

Definition 3.16 Let $i \in \{1, \dots, m\}$ and let $v_i : \mathbf{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ be the function defined by setting $v_i(0) := \infty$ and $v_i(a/b) := \rho_i(gb) - \rho_i(ga)$, where $a, b \in \mathbf{R} \setminus \{0\}$ and $g \in \mathcal{M}_{\rho_i}$ is such that $ga, gb \in \mathcal{M}_{\rho_i}$.

Observe that $v_i(a/b)$ does not depend on the choice of g because if $h \in \mathcal{M}_{\rho_i}$ is such that $ha, hb \in \mathcal{M}_{\rho_i}$ then $\rho_i(gb) - \rho_i(ga) - (\rho_i(hb) - \rho_i(ha)) = \rho_i(gbha) - \rho_i(gahb) = 0$, for all $i \in \{1, \dots, m\}$; a similar reasoning shows that if $a'/b' = a/b$, with $a, a', b, b' \in \mathbf{R} \setminus \{0\}$ then $v_i(a/b) = v_i(a'/b')$.

Lemma 3.17 *Let $i \in \{1, \dots, m\}$.*

- a) *The function $v_i : \mathbf{K} \rightarrow \mathbb{Z} \cup \{\infty\}$ is a discrete valuation of the function field $\mathbf{K} \mid \mathbb{F}$;*
- b) *If $f \in \mathbf{R}$ then $v_i(f) \geq 0$ when $f \in \mathcal{U}_{\rho_i}$ and $v_i(f) = -\rho_i(f)$ when $f \in \mathcal{M}_{\rho_i}$.*

Proof: Given $f, g \in \mathbf{K} \setminus \{0\}$ it is easy to check that $v_i(fg) = v_i(f) + v_i(g)$ and that $v_i(f) = 0$ if $f \in \mathbb{F}^*$. Since H_i has finite genus, we know that for a sufficiently large $n \in \mathbb{N}$ there are $f, g \in \mathcal{M}_{\rho_i}$ such that $\rho_i(f) = n$, $\rho_i(g) = n + 1$, hence $v_i(f/g) = 1$. Let $f = a/b, g = c/d \in \mathbf{K}$, with $a, c \in \mathbf{R}$ and $b, d \in \mathbf{R} \setminus \{0\}$, and let $h_1, h_2 \in \mathcal{M}_{\rho_i}$ such that $h_1a, h_1b, h_2c, h_2d \in \mathcal{M}_{\rho_i}$, then $v_i(f+g) = v_i((ad+bc)/bd) = \rho_i(h_1h_2bd) - \rho_i(h_1h_2ad + h_1h_2bc) \geq \min\{\rho_i(h_1h_2bd) - \rho_i(h_1h_2ad), \rho_i(h_1h_2bd) - \rho_i(h_1h_2bc)\} = \min\{\rho_i(h_1b) - \rho_i(h_1a), \rho_i(h_2d) - \rho_i(h_2c)\} = \{v_i(f), v_i(g)\}$.

Now let $f \in \mathbf{R} \setminus \{0\}$ and $g \in \mathcal{M}_{\rho_i}$ be such that $gf \in \mathcal{M}_{\rho_i}$, if $f \in \mathcal{U}_{\rho_i}$ then from (N5) and the fact that ρ_i is normalized we get $v_i(f/1) = \rho_i(g) - \rho_i(gf) \geq -\rho_i(f) = 0$; on the other hand, if $f \in \mathcal{M}_{\rho_i}$ then $v_i(f/1) = \rho_i(g) - \rho_i(gf) = -\rho_i(f)$. \square

This shows that every n -weight ρ_i on \mathbf{R} defines a valuation v_i of the function field $\mathbf{K} \mid \mathbb{F}$. These are distinct valuations (e.g. for a sufficiently large $n \in \mathbb{N}$ we may find $f_i \in \mathcal{M}_{\rho_i}$ for all $i \in \{1, \dots, m\}$ such that $v_i(f_i) = -n$ and $v_j(f_i) \geq 0$ for all $j \in \{1, \dots, m\} \setminus \{i\}$). We denote by P_i the place associated to the valuation v_i and be \mathcal{O}_{P_i} the corresponding valuation ring ($i \in \{1, \dots, m\}$).

Proposition 3.18 *For all $i \in \{1, \dots, m\}$ the place P_i has degree one (a fortiori, \mathbb{F} is the full field of constants of \mathbf{K}).*

Proof: Let $i \in \{1, \dots, m\}$, we must prove that the inclusion map $\mathbb{F} \rightarrow \mathcal{O}_{P_i}/P_i$ is surjective. Let $f = a/b \in \mathcal{O}_{P_i}$, where $a, b \in \mathbf{R}$, let $g \in \mathcal{M}_{\rho_i}$ such that $ga, gb \in \mathcal{M}_{\rho_i}$ and assume that $v_i(f) = 0$. Then $\rho_i(gb) = \rho_i(ga)$ and there exists a unique $\lambda \in \mathbb{F}^*$ such that $\rho_i(ga - \lambda gb) < \rho_i(gb)$. Let $h \in \mathcal{M}_{\rho_i}$ be such that $h(a - \lambda b), hb \in \mathcal{M}_{\rho_i}$, then $v_i(a/b - \lambda) = \rho_i(hb) - \rho_i(h(a - \lambda b)) = \rho_i(hgb) - \rho_i(hg(a - \lambda b))$, so from $\rho_i(gb) - \rho_i(ga - \lambda gb) > 0$ and property (N3) we get $\rho_i(hgb) - \rho_i(hg(a - \lambda b)) > 0$, which completes the proof. \square

We denote by $\mathbb{P}(\mathbf{K})$ the set of places of the function field $\mathbf{K} \mid \mathbb{F}$. For $P \in \mathbb{P}(\mathbf{K})$ we write \mathcal{O}_P for the corresponding valuation ring; let $\mathcal{S}(\mathbf{R}) := \{P \in \mathbb{P}(\mathbf{K}) \mid \mathbf{R} \subset \mathcal{O}_P\}$.

Proposition 3.19 $\mathcal{S}(\mathbf{R}) = \mathbb{P}(\mathbf{K}) \setminus \{P_1, \dots, P_m\}$.

Proof: First we observe that, for all $i \in \{1, \dots, m\}$ we have $P_i \notin \mathcal{S}(\mathbf{R})$, since $\mathbf{R} \subset \mathcal{O}_{P_i}$ would imply $\mathcal{M}_{\rho_i} = \emptyset$, a contradiction with the fact that ρ_i is non-trivial. Suppose by means of absurd that $\mathbb{P}(\mathbf{K}) \setminus (\mathcal{S}(\mathbf{R}) \cup \{P_1, \dots, P_m\}) \neq \emptyset$. Then, from the Strong Approximation Theorem (see [13, Thm. I.6.4]) we know that for all

$j \in \mathbb{N}$ there exists $f_j \in \mathbf{K}$ such that $v_i(f_j) = j$, for all $i \in \{1, \dots, m\}$ and $f_j \in \mathcal{O}_Q$ for all $Q \in \mathcal{S}(\mathbf{R})$, thus $f_j \in \cap_{Q \in \mathcal{S}(\mathbf{R})} \mathcal{O}_Q =: \bar{\mathbf{R}}$, the integral closure of \mathbf{R} in \mathbf{K} . Let $W := \{x \in \bar{\mathbf{R}} \mid v_i(x) > 0 \ \forall i = 1, \dots, m\}$, observe that W is an \mathbb{F} -vector space and also $W \cap \mathbf{R} = \{0\}$: in fact, if $x \in W \cap \mathbf{R}$ then $\rho_i(g) - \rho_i(gx) > 0$ for some $g \in \mathcal{M}_{\rho_i}$, thus $\rho_i(gx) < \rho_i(g)$ and from (N5) either $\rho_i(x) = 0$ for all $i \in \{1, \dots, m\}$ or $x = 0$, since $\cap_{i=1}^m \mathcal{U}_{\rho_i} = \mathbb{F}$ and $x \in W$ we must have $x = 0$. Thus $\dim_{\mathbb{F}} W \leq \dim_{\mathbb{F}} \bar{\mathbf{R}}/\mathbf{R}$ and this last dimension is finite (see e.g. [10, Lemma 8]), but $\{f_1, \dots, f_n\} \subset W$ is a linearly independent set over \mathbb{F} for all $n \in \mathbb{N}$. \square

Corollary 3.20 *\mathbf{R} is an \mathbb{F} -algebra admitting a complete set of m n -weights if and only if \mathbf{R} is the ring of regular functions of an affine geometrically irreducible algebraic curve, whose points in the closure have a total of r branches, all of them corresponding to rational places in the field of rational functions of the curve.*

Proof: The “only if” part is a consequence of the above results. As for the “if” part let \mathcal{X} be the affine curve and $\bar{\mathcal{X}}$ be its closure, if \mathcal{Y} is the normalization of $\bar{\mathcal{X}}$ and $\eta : \mathcal{Y} \rightarrow \bar{\mathcal{X}}$ is the normalization morphism then there are m rational points Q_1, \dots, Q_m in the inverse image by η of the set $\bar{\mathcal{X}} \setminus \mathcal{X}$. Now we proceed as in theorem 2.10; thus we observe that $\mathbf{R} = \cap_{Q \in \mathcal{X}} \mathcal{O}_Q$, where \mathcal{O}_Q is the local ring at $Q \in \mathcal{X}$ and denoting by v_k the discrete valuation of $\mathbb{F}(\bar{\mathcal{X}})$ associated to Q_k ($k \in \{1, \dots, m\}$) we define the function $\rho_k : \mathbf{R} \rightarrow \mathbb{N}_0 \cup \{\infty\}$ by setting $\rho_k(0) := -\infty$, $\rho_k(f) := 0$ if $v_k(f) \geq 0$ and $\rho_k(f) := -v_k(f)$ if $v_k(f) < 0$, for all $f \in \mathbf{R} \setminus \{0\}$, one may check that ρ_k is an n -weight for all $k \in \{1, \dots, m\}$. From $\cap_{k=1}^m \mathcal{U}_{\rho_k} = \mathbf{R} \cap (\cap_{k=1}^m \mathcal{O}_{Q_k}) = \mathbb{F}$ and the fact that $\mathcal{S}_k := \rho_k(\cap_{1 \leq i \leq m; i \neq k} \mathcal{U}_{\rho_i}) = \rho_k(\cap_{Q \in \mathcal{X}} \mathcal{O}_Q)$ is the Weierstrass semigroup at Q_k for all $k \in \{1, \dots, m\}$ we get that $\{\rho_1, \dots, \rho_m\}$ is a complete set of n -weights for \mathbf{R} . \square

Theorem 3.21 *Let \mathbf{R} be an \mathbb{F} -algebra that admits a complete set of m n -weights, let $\varphi : \mathbf{R} \rightarrow \mathbb{F}^n$ be a surjective morphism of \mathbb{F} -algebras and $\mathbf{a} \in \mathbb{N}_0^m$, then $C(\mathbf{a})$ is an algebraic-geometric Goppa code $C_{\mathcal{L}}(D, G)$ with G supported on m points.*

Proof: From the hypothesis on \mathbf{R} we know that there is a geometrically irreducible, projective, nonsingular curve \mathcal{Y} and points Q_1, \dots, Q_m such that $\mathbf{R} = \cap_{P \in \mathcal{Y} \setminus \{Q_1, \dots, Q_m\}} \mathcal{O}_P$. For $i \in \{1, \dots, n\}$ consider the \mathbb{F} -algebra surjective homomorphism $\pi_i : \mathbb{F}^n \rightarrow \mathbb{F}$ defined by $\pi_i(\lambda_1, \dots, \lambda_n) = \lambda_i$, then $M_i := (\pi_i \circ \varphi)^{-1}(0)$ is a maximal ideal of \mathbf{R} . Furthermore, for distinct $i, j \in \{1, \dots, n\}$ we get $M_i \neq M_j$ since φ is surjective and then exists $g_{ij} \in \mathbf{R}$ such that $(\pi_i \circ \varphi)(g_{ij}) = 0$ and

$(\pi_j \circ \varphi)(g_{ij}) \neq 0$. From [13, Prop. III.2.9] we get that there are $P_1, \dots, P_n \in \mathcal{Y}$ such that $P_i \notin \{Q_1, \dots, Q_m\}$, $M_i = \mathcal{M}_{P_i} \cap \mathbf{R}$ (where \mathcal{M}_{P_i} is the maximal ideal of \mathcal{O}_{P_i}) for all $i = 1, \dots, n$. We also get $\mathbb{F} \simeq \mathbf{R}/M_i \simeq \mathcal{O}_{P_i}/\mathcal{M}_{P_i}$ for all $i = 1, \dots, n$ hence P_1, \dots, P_n are rational points of \mathcal{Y} and we may rewrite φ as the morphism over $\mathcal{O}_{P_1}/\mathcal{M}_{P_1} \times \dots \times \mathcal{O}_{P_n}/\mathcal{M}_{P_n}$ defined by $\varphi(f) = (f + \mathcal{M}_{P_1}, \dots, f + \mathcal{M}_{P_n})$. Let $G := a_1 Q_1 + \dots + a_m Q_m$, then $L(G) \subset \mathbf{R}$ and

$$\begin{aligned} L(G) &= \{f \in \mathbf{R} : v_i(f) + a_i \geq 0 \text{ for all } i = 1, \dots, m\} = \\ &= \{f \in \mathbf{R} : -v_i(f) \leq a_i \text{ whenever } v_i(f) < 0, i = 1, \dots, m\} = \\ &= \{f \in \mathbf{R} : -v_i(f) \leq a_i \text{ whenever } f \in \mathcal{M}_{P_i}, i = 1, \dots, m\} = \\ &= \{f \in \mathbf{R} : \rho_i(f) \leq a_i \text{ whenever } f \in \mathcal{M}_{P_i}, i = 1, \dots, m\} = \\ &= \{f \in \mathbf{R} : \rho_i(f) \leq a_i, i = 1, \dots, m\} = \mathcal{L}(\mathbf{a}), \end{aligned}$$

hence $C(\mathbf{a}) = C_{\mathcal{L}}(D, G)$, where $D = P_1 + \dots + P_n$. □

References

- [1] R. E. Blahut, “AG codes without AG”, presented at 1992 IEEE Information Theory Workshop, Salvador da Bahia, Brazil, June 1992.
- [2] C. Carvalho, C. Muñuera, E. Silva and F. Torres, “Near orders and codes”, IEEE Trans. Inf. Theory, vol. 53, pt. 5, pp. 1919–1924, 2007.
- [3] C. Carvalho and F. Torres, “On Goppa codes and Weierstrass gaps at several points”, Des. Codes Cryptogr. vol. 35, n. 2, pp. 211–225, 2005.
- [4] D. Eisenbud - *Commutative Algebra with a view toward Algebraic Geometry*, Springer-Verlag, 1995.
- [5] T. Høholdt, J.H. van Lint and R. Pellikaan “Algebraic geometric codes” in *Handbook of Coding Theory*, V. Pless and W. C. Huffman eds., Elsevier, 1998, pp. 871-961, .
- [6] V. D. Goppa, “Codes on algebraic curves”, Soviet math. Dokl., vol. 24, pp. 75–91, 1981.
- [7] G. L. Matthews, “The Weierstrass semigroup of an m -tuple of collinear points on a Hermitian curve”, Lecture Notes in Computer Science vol. 2948, pp. 12-24, 2004.

- [8] M. Homma and S.J. Kim, “Goppa codes with Weierstrass pairs”, J. Pure Appl. Algebra, vol. 162, pp. 273–290, 2001.
- [9] S. J. Kim, “On the index of the Weierstrass semigroup of a pair of points on a curve”, Arch. Math. vol. 62, pp. 73–82, 1994.
- [10] R. Matsumoto, “Miuras’s Generalization fo One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan’s Generalization”, IEICE Trans. Fundamentals, vol. E82-A, no. 10, pp. 2007-2010, 1999.
- [11] C. Muñozera and F. Torres, “The structure of algebras admitting well agreeing near weights”, preprint, 2006.
- [12] E. Silva, E. Funções ordens fracas e a distância mínima de códigos geométricos de Goppa, Ph. D. Thesis, Unicamp 2004.
- [13] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.